AO 106 (Rev. 06/09) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Northern District of Oklahoma

In the Matter of the Search of
INFORMATION THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE, 1600 AMPHITHEATRE PARKWAY, MOUNTAIN VIEW, CALIFORNIA 94043

Case No. 20-mj-134-PJC ~~20-CR-00031-GKF~~

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment "A"

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized):*

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 2252(a)(2) and (b)(1)	**Receipt/distribution of a visual depiction of a minor engaged in sexually explicit conduct**
18 U.S.C. §§ 2252(a)(4)(B) and (b)(2)	**Possession of and access with intent to view a visual depiction of a minor engaged in sexually explicit conduct**
18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1)	**Receipt/distribution of child pornography**
18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2)	**Possession of and access with intent to view child pornography**

The application is based on these facts:

See Affidavit of Special Agent Dustin Carder, attached hereto.

☑ Continued on the attached sheet.

☐ Delayed notice of ___ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Dustin Carder, SA HSI
Printed name and title

Sworn to before me ~~and signed in my presence~~ telephonically.

Date: 5/29/2020

Judge's signature

City and state: Tulsa, Oklahoma

U.S. Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OKLAHOMA

IN THE MATTER OF THE SEARCH OF INFORMATION THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE, 1600 AMPHITHEATRE PARKWAY, MOUNTAIN VIEW, CALIFORNIA 94043	AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT Case No. _____

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Dustin Carder, a Special Agent (SA) with Homeland Security Investigations (HSI), being duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant[1] for information that is stored at premises controlled by Google, a provider of electronic communications service and remote computing service headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. § 2703(c)(1)(A) to require Google to disclose to the government copies of the information further described in Attachment B.

2. I have been employed as a Special Agent of the United States Department of Homeland Security, Homeland Security Investigations (HSI) in Tulsa, Oklahoma, since December 2018. I am a graduate of the Criminal Investigator Training Program

[1] A Search Warrant was previously issued for this information. However a scrivener's error in affidavit regarding the geographical coordinates made it impossible for Google to comply. Paragraphs 42 and 43 of this affidavit address this issue.

and the Homeland Security Investigations Special Agent Training Academy. As a result of my employment with HSI, my duties include, but are not limited to, the investigation and enforcement of Titles 8, 18, 19, 21, and 31 of the United States Code (U.S.C.). I am an "investigative or law enforcement officer of the United States" within the meaning defined in 18 U.S.C. § 2510(7), in that I am an agent of the United States authorized by law to conduct investigations of, and make arrests for, federal offenses.

3. As part of my duties as a HSI Special Agent, I investigate criminal violations relating to child pornography, including the production, transportation, distribution, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2251, 2252, and 2252A. I have received training in the areas of child pornography and child exploitation and have observed and reviewed numerous examples of child pornography, as defined in 18 U.S.C. § 2256, in all forms of media. I have been involved in several child pornography investigations and am familiar with the tactics used by individuals who collect and distribute child pornographic material.

4. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 2252(a)(2) and (b)(1) (receipt/distribution of a visual depiction of a minor engaged in sexually explicit conduct); and 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) (possession of and access with intent to view a visual depiction of a minor engaged in sexually explicit conduct) have been committed by Jeffrey Reetz or unknown persons. There is also probable cause to search the information described in Attachment

A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

BACKGROUND RELATING TO GOOGLE AND RELEVANT TECHNOLOGY

7. A cellular telephone or mobile telephone is a handheld wireless device used primarily for voice communication through radio signals. Cellular telephones send signals through networks of transmitter/receivers called "cells," enabling communication with other cellular telephones or traditional "landline" telephones. Cellular telephones rely on cellular towers, the location of which may provide information on the location of the subject telephone. Cellular telephones may also include global positioning system ("GPS") technology for determining the location of the device.

8. Google is an Internet company which, among other things, provides electronic communication services to subscribers. Google allows subscribers to obtain email accounts at the domain name gmail.com. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information. Therefore, the computers of Google are likely to contain stored electronic communications (including retrieved and unretrieved email for Google subscribers) and information concerning subscribers and their use of Google services, such as account access information, email transaction information, and account application information. In my training and experience, such information

may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

9. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that even if subscribers insert false information to conceal their identity, I know that this information often provide clues to their identity, location or illicit activities.

10. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of login (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

11. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. Further, information maintained by the email provider can show how, where, and when the account was accessed or used. Based on my training and experience, I have learned that Google also maintains records that may reveal other Google accounts accessed from the same electronic device, such as the same computer or mobile device, including accounts that are linked by Hypertext Transfer Protocol (HTTP) cookies, which are small pieces of data sent from a website and stored in a user's Internet browser.

12. Google has developed an operating system for mobile devices, including cellular phones, known as Android. Nearly every cellular phone using the Android operating system has an associated Google account and users are prompted to add a Google account when they first turn on a new Android device.

13. Based on my training and experience, I have learned that Google collects and retains location data from Android-enabled mobile devices when a Google account user has enabled Google location services. The company uses this information for location-based advertising and location-based search results. This information is derived from sources including GPS data, cell site/cell tower information, and Wi-Fi access points. This location data is retained by Google in the Northern District of California, in Mountain View, California.

14. Location data can assist investigators in understanding the timeline and physical location of an Android-enabled mobile device relating to the crime under investigation, when a

Google user has enabled Google location services. This timeline and device physical location information may tend to either inculpate or exculpate the account owner. Affiant believes that that google location services would help establish venue. Additionally, information stored at the user's account may further indicate the physical location of the account user at a particular time (e.g., location information integrated into an image or video sent via email).

15. This search warrant seeks to collect the above-described location data obtained by Google in an effort to determine what devices were in or near **9574 East Highway 20, Claremore, Oklahoma**, in the Northern District of Oklahoma, on numerous dates and times, as further described in paragraph 32. The dates and times listed in paragraph 32 are when a known commercial child exploitation website, described in paragraph 16, was accessed from a laptop found at **9574 East Highway 20, Claremore, Oklahoma** during the execution of a previous federal search warrant on January 23, 2020.

PROBABLE CAUSE

16. In March 2012, HSI Phoenix initiated an investigation into a fee-based, members-only website, "Website M,"[2] after a consensual interview with a suspect in a child exploitation investigation. The interview resulted in HSI agents assuming this individual's online identity on "Website M," a commercial child exploitation website (CEW). Additionally, Special Agents (SAs) were able to take over the e-mail account the suspect utilized when he registered for the

[2] Law enforcement knows the actual name of Website M. However, the investigation into users of Website M remains ongoing, and public disclosure of Website M's actual name would potentially alert its members to the investigation, likely provoking members to notify other members of the investigation, to flee, and/or to destroy evidence. Accordingly, to preserve the confidentiality and integrity of the ongoing investigation, the actual name and other identifying details of Website M remain undisclosed in this affidavit.

CEW. Results from the preliminary investigation indicated that the site was being hosted on a server physically located in India, and the website claimed to offer 600,000 images and 400 hours of video, all of which could be downloaded for a fee as compressed, encrypted files (.RAR files). A review of the images and videos displayed on the website indicate that approximately one-half of the images and more than one-half of the videos advertised depict prepubescent and pubescent males and females engaged in sexual activity with adults and/or posed in a sexually explicit manner. Passwords to decrypt the files were available for an average fee of $83.00. Due to this site being "members-only" it is impossible to access it without an active account.

17. A user can only locate and access Website M if the user knows its current web address. Once the user enters the correct web address, a box appears that requires the user to enter a "username" and "password." The user cannot access the site without first entering that information. Once the user enters a valid username and password, Website M's home page appears. The opening page depicts nude anime (i.e., drawings, sketches or cartoons) characters lasciviously displaying their genitals. The term "Private Club" also appears on the home page.

18. Several interviewed Website M members have told agents that they received an e-mail message inviting them to join the site and set up a username and password after they purchased child erotica from another website. Following that purchase, they received a sample image of child pornography[3] along with the question "Are you interested in seeing more of this?"

[3] "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

If the individual gave a positive indication that they were interested in seeing more of those images, Website M sent them another email with instructions of how to access and join the website.

19. After gaining access to Website M by using a cooperating individual's username and login, HSI Phoenix agents determined that it advertises files of child pornography for purchase. Once logged in as a member, the user sees the names of folders available for purchase, which contain previews or samples of images contained in the folders. As of March 2012, the website advertised that it offered 600,000 images and 400 hours of video. Such images and videos are organized into folders, the contents of which can be accessed after downloading them by purchasing a password. At all times relevant to this investigation, Website M hosted its content on a server physically located outside of the United States.

20. Throughout HSI's investigation, Website M has typically charged between $40 USD and $110 USD to purchase the password for encrypted archive files containing multiple images and/or videos of child pornography and child erotica. The majority of archive files cost $89 USD[4]. Once downloaded, the user can "decrypt" the selected archive file by entering in the purchased password to reveal multiple images and/or video files. HSI Phoenix Special Agents have made undercover purchases or accessed several archive files available for purchase, which revealed that most of the archive files contained between 500 and 2,000 image and/or video files, the majority of which are child pornography.

21. Investigating agents also found that Website M allows members to preview "samples" of the images/videos contained in an archive folder prior to purchase. Investigating

[4] A digital archive file is used to store multiple files within a single, compressed file, which can make it easier to store and transmit numerous files at the same time. File extensions associated with digital archive files include ".rar" and ".zip."

agents visited Website M and previewed more than 100 sample folders. Agents found that the majority of the images and videos found in the sample or preview folders depicted apparent minors, and many depicted what appeared to be pre-pubescent minors engaged in sexual activity with adults and/or posed in a sexually explicit manner.

22. Over the course of their investigation, which has involved previewing "samples" and then downloading multiple archive files via Website M, investigating agents have found that the "sample" images and/or video screenshots corresponded to the full sets of image and video files contained in downloaded archive files.

23. After selecting an archive file for purchase, the member pays for its password via credit card. Website M then automatically sends an email to the member with the encryption password for the archive. The member must first download the archive file to a digital device and enter that password to decrypt and de-compress it.

24. Through years of investigation, research, undercover purchases of child pornography from Website M, the service of legal process, and working with foreign governments, HSI identified numerous targets in the United States via the capture of IP addresses and summons results from payment processors for Website M. One of the targets was identified as Jeffrey Reetz at **9574 East Highway 20, Claremore, Oklahoma**. This identification was made through responses to legal process served to the Website M payment processor and Internet Service Providers for IPs captured during purchases.

25. For each of the purchases on Website M, the user must enter the email address to which the site sent the auto-generated receipts and passwords for purchases made on Website M. The email address that the individual provided on each purchase was "lareetz@msn.com." The name the user provided for each purchase was Jeffrey Reetz.

26. At least one of the U.S. payment processors for Website M provided the IP addresses related to particular user transactions. One of the IP addresses related to Reetz' transactions was 108.243.235.60. A query of the American Registry for Internet Numbers ("ARIN") online database revealed that IP address 108.243.235.60 was registered to AT&T.

27. On May 24, 2018, the U.S. Department of Homeland Security issued an administrative summons to AT&T seeking subscriber information concerning the above IP address. A review of the results obtained on June 4, 2018, identified the physical address as 9574 East Highway 20, Claremore, Oklahoma. AT&T also provided Reetz' email on the return information as "lareetz@msn.com."

28. HSI Phoenix discovered that Reetz made fifteen (15) purchases of child pornography from Website M between January 2017 and November 2018. The total number of files purchased by Reetz was over 39,000. HSI Phoenix was able to provide these files to me. On November 25, 2019, after reviewing and categorizing the files, it was determined that there were over 9,000 images and videos of child pornography. Of those 9,000+ images/videos, over 2,900 depicted infant/toddler exploitation and over 800 depicted child pornography containing sadomasochism, bondage, and other acts of violence.

29. On January 23, 2020, HSI Special Agents (SA), Task Force Officers (TFO), Officers from the Tulsa Police Department Cyber Crimes Division, and Investigators from the Oklahoma Department of Corrections (DOC) executed a federal search and seizure warrant at the residence of Jeffrey Reetz at **9574 East Highway 20**, Claremore, Oklahoma, in the Northern District of Oklahoma. The warrant was obtained in the Northern District of Oklahoma, which was signed by U.S. Magistrate Judge Frank H. McCarthy. The search and seizure warrant was for

evidence relating to child exploitation and a prohibited person in possession of firearms and ammunition.

30. As a result of the search warrant, agents seized numerous items including a Hewlett Packard (HP) Pavilion Entertainment PC laptop (hereinafter "HP laptop"), Model: DV5, Serial: CNF8288603, a Dell OptiPlex computer tower (serial # F1Q6KN1), and a Samsung Galaxy S9 (Phone number 918-406-3041, ICCID 89011203002449694118) from the residence.

31. Forensic analysis of the devices was conducted by a HSI Computer Forensic Analyst (CFA). I further reviewed those analyses and the images/videos found on the devices. I discovered that on the HP laptop, approximately 8,600 images and videos of child pornography were found; on the Dell OptiPlex computer tower, approximately 600 images of child pornography were found. The Samsung Galaxy S9, belonging to Jeffrey Reetz, was found to be utilizing the Android operating system, as described above in paragraphs 12-13. I know from my experience that individuals who possess android phones such as the Galaxy S9 keep that phone in their immediate possession, or nearby, at all times.

32. Additional analysis of the forensic data revealed that records of contact with Website M were found on the HP laptop for the following dates and time frames:

a. January 19, 2017 between 10:10 AM and 10:20 AM (CST)

b. January 23, 2017 between 11:45AM and 11:55 AM (CST)

c. January 24, 2017 between 8:15 AM and 8:25 AM (CST)

d. January 25, 2017 between 9:35 AM and 9:45 AM (CST)

e. January 27, 2017 between 12:35 PM and 12:45 PM (CST)

f. May 24, 2017 between 11:45 AM and 11:55 AM (CST)

g. December 26, 2017 between 11:25 AM and 11:35 AM (CST)

h. January 3, 2018 between 5:25 PM and 5:35 PM (CST)

i. August 23, 2018 between 2:15 PM and 2:25 PM (CST)

j. August 27, 2018 between 4:00 PM and 4:10 PM (CST)

k. September 6, 2018 between 5:10 PM and 5:20 PM (CST)

l. September 8, 2018 between 9:40 PM and 9:50 PM (CST)

m. September 23, 2018 between 9:10 PM and 9:20 PM (CST)

n. October 6, 2018 between 12:20 PM and 12:30 PM (CST)

o. October 13, 2018 between 4:35PM and 4:45 PM (CST)

p. November 2, 2018 between 10:35 PM and 10:45 PM (CST)

q. November 7, 2018 between 2:15 PM and 2:25 PM (CST)

r. November 8, 2018 between 7:55 PM and 8:05 PM (CST)

s. August 15, 2019 between 11:25 AM and 11:35 AM (CST)

t. November 6, 2019 between 9:35 AM and 9:45 AM (CST)

u. November 7, 2019 between 10:05 AM and 10:15 AM (CST)

v. November 13, 2019 between 9:25 AM and 9:35 AM (CST)

w. December 4, 2019 between 9:20 AM and 9:30 AM (CST)

x. December 6, 2019 between 9:45 AM and 9:55 AM (CST)

y. December 9, 2019 between 9:15 AM and 9:25 AM (CST)

z. December 12, 2019 between 10:00 AM and 10:10 AM (CST)

aa. December 13, 2019 between 10:20 AM and 10:30 AM (CST)

bb. December 17, 2019 between 10:15 AM and 10:25 AM (CST)

cc. December 18, 2019 between 9:25 AM and 9:35 AM (CST)

dd. January 3, 2020 between 9:05 AM and 9:15 AM (CST)

ee. January 16, 2020 between 10:00 AM and 10:10 AM (CST)

ff. January 21, 2020 between 9:45 AM and 9:55 AM (CST)

33. Reetz was interviewed at the time of the execution of the search warrant, after waiving his Miranda Rights. Reetz vehemently denied ever looking at, accessing, or downloading child pornography from any website. Reetz stated that the only person at the residence who had access to the WiFi during the known purchases of child pornography was his ex-wife, Danielle Morris. I attempted to locate Danielle Morris for an interview, but learned she moved to California and I was unable to make contact with her by phone.

34. It is common knowledge that in today's society, most individuals carry their cellular phone or smartphone on their person, or it is near them at almost all times. As described in paragraph 31, Reetz' Samsung phone seized at his residence during the search warrant on January 23, 2020, was found to be utilizing the Android operating system. The HP laptop was found in Reetz' vehicle inside his garage contained in a briefcase with numerous passports and or financial/identity documents belonging to Reetz. It is believed that Reetz traveled with the HP laptop from home to work and work to home.

35. As described in this affidavit, location data can assist investigators in understanding the timeline and physical location of an Android-enabled mobile device relating to the crime under investigation, when a Google user has enabled Google location services. The ultimate goal of this search warrant is to identify devices that were at or near 9574 East Highway 20, Claremore, Oklahoma on the aforementioned dates and times during which Website M was accessed on the HP laptop, so that owner/account information can later be sought from Google for those identified devices, which will inculpate or exculpate Reetz or another individual as the one who accessed Website M.

36. I am only seeking to identify devices that were at or near 9574 East Highway 20, Claremore, Oklahoma and not Reetz' business because the business has approximately 35-40 employees and sits next to a roadway and other businesses. In my training and experience, those who access and view child pornography do so from their homes or other places where they have a greater expectation of privacy.

37. Reetz' residence sits on approximately 26 acres of land and his residence is nearly 450 feet from the roadway. The neighbor to the west is a church and the neighbor to the east is approximately 750 feet away through a wood line. The neighbor to the north is nearly 800 feet away and approximately 20 acres of land is south of the residence[5].

38. This search warrant seeks location information related to GPS, WiFi or Bluetooth sourced location history data generated from devices that reported a location within the geographical area around 9574 East Highway 20, Claremore, Oklahoma 74017, in the Northern District of Oklahoma, described by the following points of latitude/longitude (see Attachment A for photograph as well as photograph on the following page):

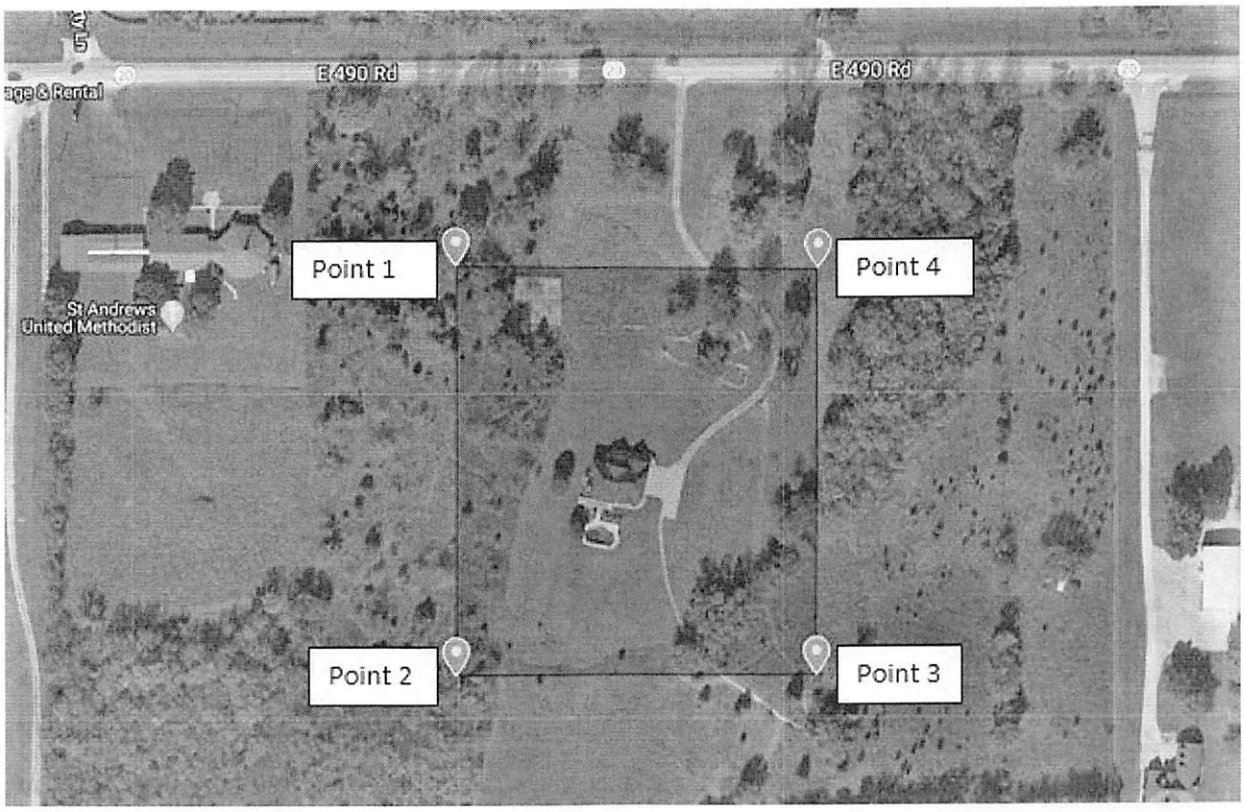
Point 1: 36.3067, -95.65797

Point 2: 36.3053, -95.65796

Point 3: 36.3053, -95.65644

Point 4: 36.30669, -95.65644

[5] All distances to nearby homes, church, roadway were calculated with Google Maps. Google Maps is a web mapping service developed by Google. It offers satellite imagery, aerial photography, street maps, 360° interactive panoramic views of streets, real-time traffic conditions, and route planning for traveling by foot, car, bicycle and air, or public transportation. Google Maps also allows users to measure distances from one point to another.



39. I determined these four points above by utilizing Google MyMaps[6] and creating a square around 9574 East Highway 20, Claremore, Oklahoma, which is in the center of the square pictured above. I utilized Google MyMaps to determine the latitudinal and longitudinal coordinates of each point, as listed in paragraph 38. Due to the nearby highway and church, I wanted to contain the search for location/device information to this determined area so that uninvolved parties driving by the residence or attending the church would not be included in the results. There are no other businesses or homes located within the four points set out above other

[6] Google MyMaps is online software provided by Google that allows users to create custom maps, add points of reference, draw shapes on maps, create maps from spreadsheets, and personalize the map with icons and colors. Users are also able to add photos and videos to any place.

than the residence of 9574 East Highway 20, Claremore, Oklahoma which was the home of Jeffrey Reetz.

40. This search warrant also seeks identifying information for Google Accounts associated with the responsive location history data, as further described in Attachment B.

CONCLUSION

41. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on Google who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

42. On April 3, 2020, I originally obtained a federal search warrant in the Northern District of Oklahoma for this device geolocation data as collected by Google. The warrant was signed by US Magistrate Judge Paul J. Cleary. On May 28, 2020, I was contacted by a Google representative advising me that I had made an error on the first search warrant by listing Point 1 and Point 4 as the same coordinates, thus changing the polygon from a square to a triangle. Google stated that I would need an amended search warrant to obtain the requested data.

43. After receiving this information, I recreated the polygon utilizing Google MyMaps, as instructed by the Google representative, and obtained the proper coordinates of Points 1-4, as listed in paragraph 38 and Attachment A.

Respectfully submitted,

Dustin Carder
Special Agent
Homeland Security Investigations

Subscribed and sworn to ~~before~~ telephonically me on May 29th, 2020

UNITED STATES MAGISTRATE JUDGE
NORTHERN DISTRICT OF OKLAHOMA

ATTACHMENT A

Property To Be Searched

This warrant is directed to Google LLC, headquartered at 1600 Amphitheatre Parkway, Mountain View, California, and applies to (1) GPS, WiFi or Bluetooth sourced location history data generated from devices that reported a location within the geographical region bounded by the following latitudinal and longitudinal coordinates, dates, and times ("Initial Search Parameters") and (2) identifying information for Google Accounts associated with the responsive location history data:

Dates & Time Periods (including time zone):

a) January 19, 2017 between 10:10 AM and 10:20 AM (CST)

b) January 23, 2017 between 11:45AM and 11:55 AM (CST)

c) January 24, 2017 between 8:15 AM and 8:25 AM (CST)

d) January 25, 2017 between 9:35 AM and 9:45 AM (CST)

e) January 27, 2017 between 12:35 PM and 12:45 PM (CST)

f) May 24, 2017 between 11:45 AM and 11:55 AM (CST)

g) December 26, 2017 between 11:25 AM and 11:35 AM (CST)

h) January 3, 2018 between 5:25 PM and 5:35 PM (CST)

i) August 23, 2018 between 2:15 PM and 2:25 PM (CST)

j) August 27, 2018 between 4:00 PM and 4:10 PM (CST)

k) September 6, 2018 between 5:10 PM and 5:20 PM (CST)

l) September 8, 2018 between 9:40 PM and 9:50 PM (CST)

m) September 23, 2018 between 9:10 PM and 9:20 PM (CST)

n) October 6, 2018 between 12:20 PM and 12:30 PM (CST)

o) October 13, 2018 between 4:35PM and 4:45 PM (CST)

p) November 2, 2018 between 10:35 PM and 10:45 PM (CST)

q) November 7, 2018 between 2:15 PM and 2:25 PM (CST)

r) November 8, 2018 between 7:55 PM and 8:05 PM (CST)

s) August 15, 2019 between 11:25 AM and 11:35 AM (CST)

t) November 6, 2019 between 9:35 AM and 9:45 AM (CST)

u) November 7, 2019 between 10:05 AM and 10:15 AM (CST)

v) November 13, 2019 between 9:25 AM and 9:35 AM (CST)

w) December 4, 2019 between 9:20 AM and 9:30 AM (CST)

x) December 6, 2019 between 9:45 AM and 9:55 AM (CST)

y) December 9, 2019 between 9:15 AM and 9:25 AM (CST)

z) December 12, 2019 between 10:00 AM and 10:10 AM (CST)

aa) December 13, 2019 between 10:20 AM and 10:30 AM (CST)

bb) December 17, 2019 between 10:15 AM and 10:25 AM (CST)

cc) December 18, 2019 between 9:25 AM and 9:35 AM (CST)

dd) January 3, 2020 between 9:05 AM and 9:15 AM (CST)

ee) January 16, 2020 between 10:00 AM and 10:10 AM (CST)

ff) January 21, 2020 between 9:45 AM and 9:55 AM (CST)

Target Location:

Geographical area around 9574 East Highway 20, Claremore, Oklahoma 74017 identified as a polygon defined by the following latitude/longitude coordinates and connected by straight lines:

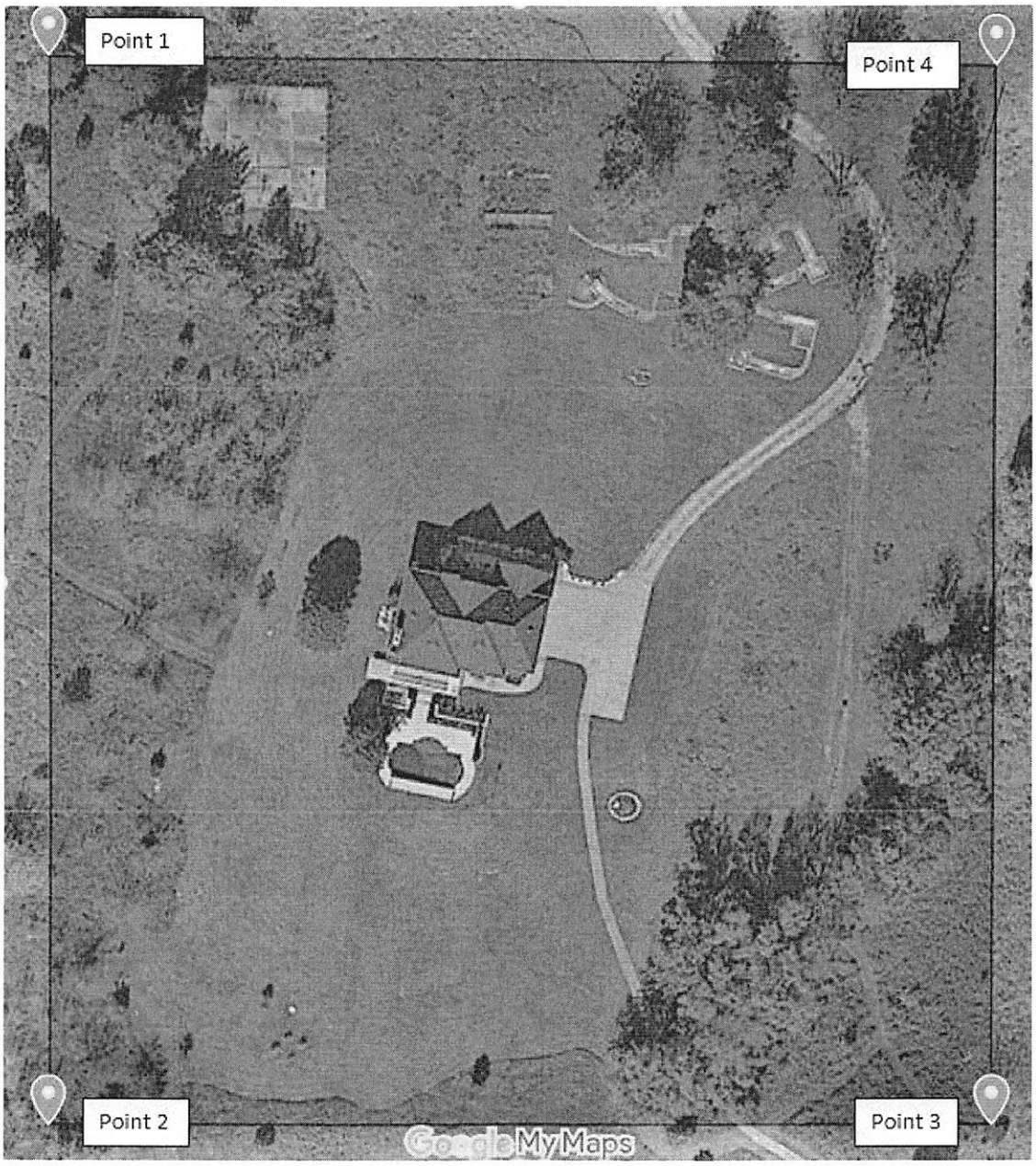
Point 1: 36.3067, -95.65797

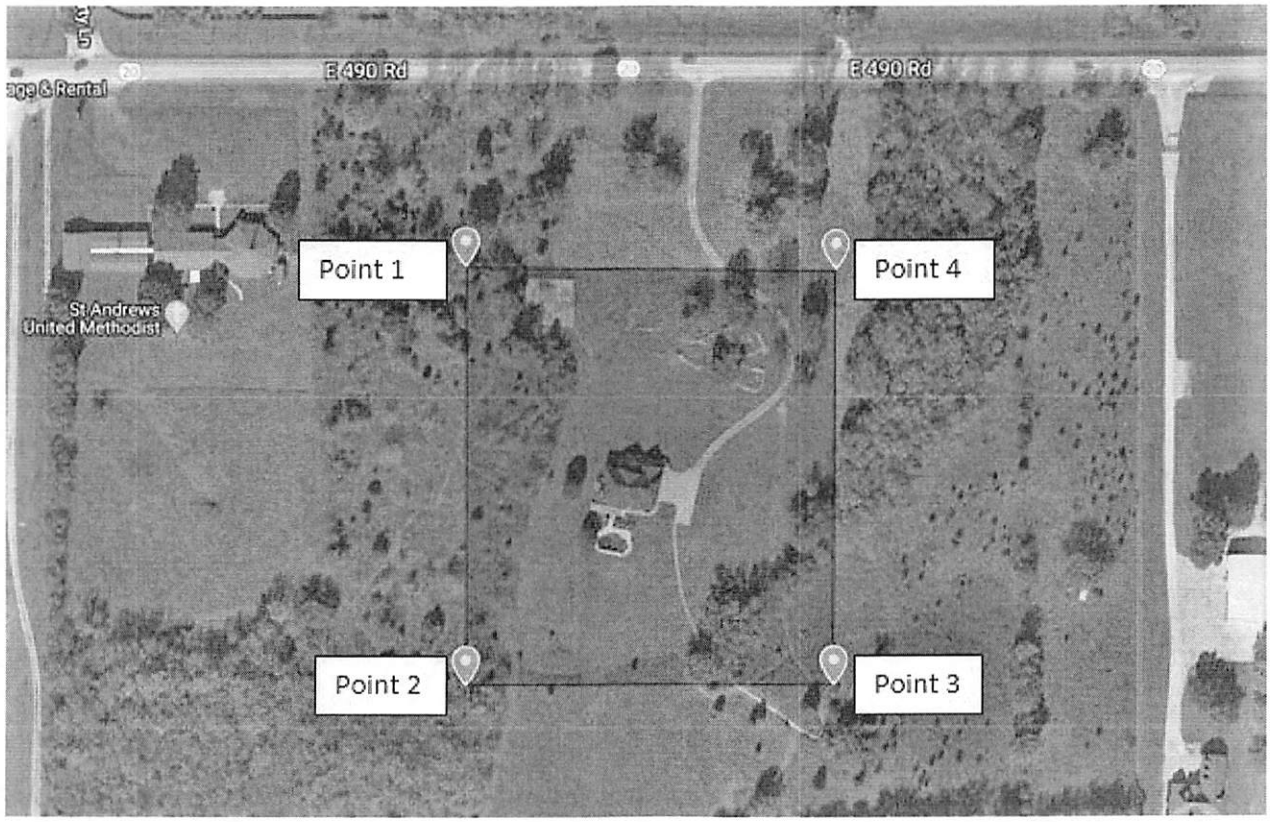
Point 2: 36.3053, -95.65796

Point 3: 36.3053, -95.65644

Point 4: 36.30669, -95.65644

Please see the **Target Location Reference Images** below and on following page:




E 490 Rd
E 490 Rd
Point 1
Point 4
Point 2
Point 3
St Andrews
United Methodist

ATTACHMENT B

Items To Be Seized And Searched

I. Information to be disclosed by Google

Google shall provide responsive data (as described in Attachment A) pursuant to the following process:

1. Google shall query location history data based on the Initial Search Parameters (as described in Attachment A).

2. For each location point recorded within the Initial Search Parameters, Google shall produce anonymized information specifying the corresponding unique device ID, timestamp, coordinates, display radius, and data source, if available (the "Anonymized List").

3. Law enforcement shall review the Anonymized List to remove devices that are not relevant to the investigation, for example, devices that were not in the location for a sufficient period of time. If additional location information for a given device ID is needed in order to determine whether that device is relevant to the investigation, law enforcement may request that Google provide additional location coordinates for the Time Period that fall outside of the Target Location. These contextual location coordinates may assist law enforcement in identifying devices that were located outside the Target Location, were not within the Target Location for a long enough period of time, were moving through the Target Location in a manner inconsistent with the facts of the underlying case, or otherwise are not relevant to the investigation.

4. For those device IDs identified as relevant pursuant to the process described above, law enforcement may request that Google Provide identifying information, as defined in 18 U.S.C. § 2703(c)(2), for the Google Account associated with each identified device ID.